Key Management Infrastructure (KMI) Capability Increment 2 (CI-2)

(version 2.0)

Date: 2014-09-03

CYBER CoE - Signal School

This page intentionally left blank

Table Of Contents

6.1.2 Architectures and Standards Component

6.1.3 Management, Evaluation, and Resource (MER) Processes Component

6.1.3.1 Management

6.1.3.1.1 Strategic Planning

6.1.3.1.2 Concept Development and Experimentation (CD&E)

6.1.3.1.3 Research and Studies

6.1.3.1.4 Policy and Guidance

6.1.3.1.5 Requirements Generation

6.1.3.1.6 Synchronization

6.1.3.1.7 Joint Training Support

6.1.3.2 Evaluation

6.1.3.2.1 Quality Assurance (QA)

6.1.3.2.2 Assessments

6.1.3.2.3 Customer Feedback

6.1.3.2.4 Lessons Learned/After-Action Reviews (AARs)

6.1.3.3 Resource

7.0 Operational Training Domain

7.1 Operational Training Concept and Strategy

7.1.1 Product Lines

7.1.1.1 Training Information Infrastructure

7.1.1.1.1 Hardware, Software, and Communications Systems

7.1.1.1.2 Storage, Retrieval, and Delivery

7.1.1.1.3 Management Capabilities

7.1.1.1.4 Other Enabling Capabilities

7.1.1.2 Training Products

7.1.1.2.1 Courseware

7.1.1.2.2 Courses

7.1.1.2.3 Training Publications

7.1.1.2.4 TSP

7.1.1.3 TADSS

7.1.1.3.1 Training Aids

7.1.1.3.2 Training Devices

7.1.1.3.3 Simulators

7.1.1.3.4 Simulations

7.1.1.3.5 Instrumentation

7.1.1.4 Training Facilities and Land

7.1.1.4.1 Ranges

7.1.1.4.2 Maneuver Training Areas (MTA)

7.1.1.4.3 Classrooms

7.1.1.4.4 CTCs
7.1.1.4.5 Logistics Support Areas
7.1.1.4.6 Battle Command Training Centers (BCTC)
7.1.1.5 Training Services
7.1.1.5.1 Management Support Services
7.1.1.5.2 Acquisition Support Services
7.1.1.5.3 General Support Services
7.1.2 Architectures and Standards Component
7.1.2.1 Operational View (OV)
7.1.2.2 Systems View (SV)
7.1.2.3 Technical View (TV)
7.1.3 Management, Evaluation, and Resource (MER) Processes Component
7.1.3.1 Management
7.1.3.1.1 Strategic Planning
7.1.3.1.2 Concept Development and Experimentation (CD&E)
7.1.3.1.3 Research and Studies
7.1.3.1.4 Policy and Guidance
7.1.3.1.5 Requirements Generation
7.1.3.1.6 Synchronization
7.1.3.1.7 Joint Training Support
7.1.3.2 Evaluation
7.1.3.2.1 Quality Assurance (QA)
7.1.3.2.2 Assessments
7.1.3.2.3 Customer Feedback
7.1.3.2.4 Lessons Learned/After-Action Reviews (AARs)
7.1.3.3 Resource Processes
8.0 Self-Development Training Domain
8.1 Self-Development Training Concept and Strategy
8.1.1 Product Lines
8.1.1.1 Training Information Infrastructure
8.1.1.1.1 Hardware, Software, and Communications Systems
8.1.1.1.2 Storage, Retrieval, and Delivery
8.1.1.1.3 Management Capabilities
8.1.1.1.4 Other Enabling Capabilities
8.1.1.2 Training Products
8.1.1.2.1 Courseware
8.1.1.2.2 Courses
8.1.1.2.3 Training Publications
8.1.1.2.4 Training Support Package (TSP)

This System Training Plan (STRAP) is preliminary.
Front end analysis (mission, task, job) is ongoing. CYBER CoE - Signal School will amend and update this STRAP as details solidify.

CYBER CoE - Signal School is the proponent for this STRAP.
Send comments and recommendations directly to: Gerald F Evans

Comm: 706-791-8132
DSN: 780-8132
Email:
Mailing address:
New Systems Integration Branch (NSIB)
8th Avenue - Moran Hall Bldg #29803
Augusta, GA 30905

1.0 System Description

Key Management Infrastructure (KMI) Capability Increment-2 (CI-2) will be a single, automated, network-accessible, electronic-based Key Management (KM) and predominantly electronic cryptographic product delivery infrastructure. It will provide Net Centric, reliable, timely, and secure Communications Security (COMSEC) material management (authorization, validation, accounting, planning, key management, CRYPTONET management) and distribution. It will additionally provide the means for secure ordering, generation, production, distribution, management and auditing of cryptographic products (e.g., asymmetric key, symmetric keys, manual cryptographic systems and cryptographic applications).

KMI CI-2 will support requirements for all cryptographic material needed to achieve information superiority. For example, KMI CI-2 will provide support to the following systems/services:

- Identification Friend or Foe (IFF)
- Electronic Commerce and Electronic Data Interchange (EDI) with government and commercial partners
- Secure electronic mail
- Wide-Area Network (WAN) security
- Wired Telephony
- Wireless Local Area Network (LAN)/data device encryption
- Video teleconferencing
- Virtual Private Network (VPN) technology
- Backbone and link encryption
- Secure tactical radio systems
- Mobile radio and cell phones
- Space systems
- Global Positioning System (GPS)
- Integrated Broadcast System (IBS)
- Global Broadcast Service (GBS)
- Weapon system Mission Planning Systems (MPS)
- Transformational Satellite Communications System (TSAT)
- Advanced Extra High Frequency (AEHF) Satellite System
- Joint Tactical Radio System (JTRS)
- Secure voice systems
- DODIN Bandwidth Expansion (DODIN BE)
- Warfighter Information Network - Tactical (WIN-T)

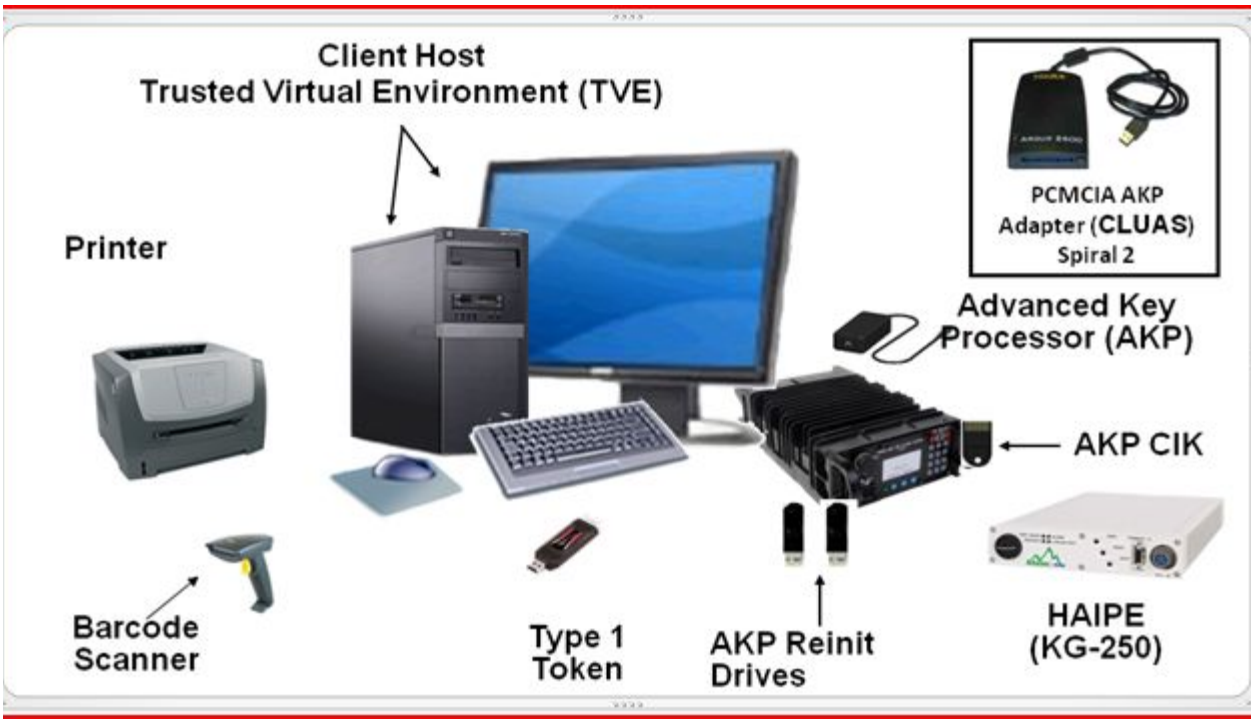
FUE for Spiral 2 is on or about 4QFY14

Management Client (MGC). The MGC is a configuration of a client node that enables an external KMI Operational Manager to manage KMI products and services by either (1) accessing a Primary Service Node (PRSN), or (2) exercising locally provided capabilities. An MGC consists of a client platform, High Assurance Internet Protocol Encryptor (HAIPE), and an Advanced Key Processor (AKP). Other peripheral devices include a printer, bar code scanner, AKP Reinit Drives, AKP Crypto Initialization Key (CIK), keyboard, monitor, mouse, Type 1 Token, and Personal Computer Memory Card International Association (PCMCIA) AKP Adapter.

The Client Host Only (CHO) is a KMI Client without the AKP. The CHO reduces the overall cost to KMI customers for roles that do not need a cryptographic coprocessor. The CHO will be able to: Support Product Ordering & Management, Inventory Management, and Downloading encrypted key. The CHO will not be able to: Decrypt, encrypt, locally generate key or communicate directly with another KM Client Node.

KMI Roles: Controlling Authority, Command Authority, KOAM with no need to decrypt key, Registration Manager, and Enrollment Manager.

[[1747|img]]



Components of the Management Client

2.0 Target Audience

General Purpose Users (GPU) will come from existing Army Military Occupational Specialties (MOS), Warrant Officer Specialty Codes (WOSC), Officer Functional Areas (FA) and Areas of Concentration (AOC), Air Force Specialty Codes (AFSC), Navy Enlisted Classification (NEC), Marine Corp Occupational Specialties (MOS), DoD civilian employees, and contractor personnel.

Training target audience will consist of new KMI users, the current EKMS user community, plus personnel identified as trainers for their respective Services as well as certain infrastructure support personnel.

The target audience will perform the following roles : KMI Operating Account (KOA) Manager (KOAM), System Administrator (SA), System Security Officer (SSO), Controlling Authority (CONAUTH) and Command Authority (CMDAUTH). Registration personnel are a new facet of the target audience. KMI users must have an active Secret clearance.

Some individuals may be assigned several KMI roles in order to perform all functions their organization associates with their position. The following table outlines pertinent external management and non-management roles.

[[img|1179]]

External operational management roles are assigned to managers within the Army KMI infrastructure or a supporting Army KOA. These managers are primarily concerned with registration, enrollment, and product management functions within the Army KMI, or some sub-unit of such an organization.

External management roles are assigned to KMI operational managers in customer organizations who:

- Connect to KMI exclusively across network interfaces to the PRSN
- Receive their privileges through the KMI manager enrollment process
- Authenticate themselves to KMI using KMI manager credentials
- Have their access to KMI mediated by role, rule, and approval

based access controls

Army network/key managers in the role of product managers in CI-2 are responsible for defining required key and cryptographic products, assigning key attributes and product parameters, and for managing the order and distribution of those products, either directly or by assigning responsibilities to supporting/subordinate users in the product requester role .

A CONAUTH is an external manager responsible for determining what key products are needed operationally to enable required cryptonets and for identifying individuals responsible for more detailed management of those products.

The CMDAUTH encompasses oversight functions required for management of asymmetric key products:

- Request Partition and Department Agency Organization (DAO) Codes. The DAO code is a unique identifier of a specific department, agency, or organization with which a key is associated. DAO codes are used to support Privilege Establishment Requests (PER) to support asymmetric key ordering. A DAO simply says who you are and authorizes the order of modern key in support of your entity. A CMDAUTH receives notice from a Product Requester, typically out-of-band, that a new DAO code or partition code is needed. Working at a Management Client (MGC), the CMDAUTH connects to a Primary Service Node (PRSN) and requests that a new code be assigned. The PRSN assigns a DAO code or partition code for the product and designates the code to be under the control of the requesting CMDAUTH.
- Allocate Codes to Product Requesters. The CMDAUTH selects one or more user identities that have previously been enrolled as Product Requesters, and authorizes those users to request asymmetric products containing the partition codes and DAO codes that the CMDAUTH has established.
- Approve Product Requests. In some cases, it may be necessary to require an approval step in the ordering of asymmetric products. The CMDAUTH is responsible both for identifying such a need, and for serving as the approving manager when such approvals are required for products that are managed by the CMDAUTH.

A Product Requester (PR) is an external manager responsible for requesting products and services and maintains the Account Distribution Profile (ADP). PR must be enrolled as Manager, and his privileges for ordering specific KMI CI-2 products are then defined by the Product Manager (PM) responsible for those products. The PR who orders asymmetric products perform a function equivalent to User Representatives in existing FIREFLY key management processes.

A KOA Manager (KOAM) is an external manager responsible for operation of one or more KOAs. KOAMs are the KMI equivalent of COMSEC custodians/COMSEC Account Managers (CAM). A KOAM manages distribution of KMI products to assigned ECUs, fill devices, and AKPs that are assigned to the manager's KOA. The KOAM designates and registers KOA Agents.

Registration Managers (RM) are the external managers responsible for making KOAs, people, and devices known to KMI. Each of the four registration functions below is addressed with a distinct registration manager role.

KOA RM maintains KOA registration information. This information is retained in a "data store" internal to KMI; information elements common to KMI and EKMS are synchronized between KMI registration "data store" and the EKMS directory server.

Since all KOAs will be CAMs in KMI, close coordination is needed between EKMS Registration Authorities (RA) and the KOA RM. For military services, the EKMS RA is located with the Tier 1 system; the EKMS RA will be enrolled as a KOA RM and provided an MGC and manager credentials so he can perform both functions.

Personnel Registration Managers (PRM) - The PRM basic functions are:

- Register KMI personnel
- Add, modify, update, and delete registration data
- Work with local sponsor authority to obtain information required to establish an individual's Type 1 identity
- Verify need for identity
- Enter required registration information into KMI using an MGC

Device Registration Manager (DRM) - DRM basic functions are:

- Register fill devices and ECUs in KMI

- Initialize ECUs, Type 1 Tokens, and any other KMI devices in KMI
- Request initial keys for fill devices and ECUs (e.g., seed key)

Local Type 1 Registration Authority (LT1RA): The LT1RA endorses and provisions KMI Aware Devices and personalizes KMI Manager Tokens. There are LT1RAs for both personnel (PLT1RA) and devices (DLT1RA).

PLT1RA basic functions are:

- Perform face-to-face verification of the identity for the user receiving the Type 1 certificate and token
- Process individuals to obtain their Type 1 Token
- Use the MGC to initiate a certificate request and download a Type 1 certificate onto a token

DLT1RA basic functions are:

- Verify the existence and condition of KMI Aware Devices
- Approve devices' infrastructure seed key conversion
- Use the MGC to initiate a request for Type 1 public key certificate
- Register and endorse KMI Aware Devices (i.e. ECUs, Type 1 Tokens, and Advanced Key Processors (AKP))

Enrollment Manager (EM) is a security-sensitive role. The EM determines what other KMI managers may or may not do. The EM cannot be a PRM or a PLT1RA. Enrollment Managers basic functions are:

- Assign KMI User identities to KMI management roles
- Assign rule-based attributes to KMI manager identities
- Assign privileges to a Type 1 identity that has been issued for use in KMI

User Support Managers:

- Provide a mixture of customer organization-specific help staff (external) and KMI-wide help staff (internal)
- Provide technical support to KMI users
- Provide customer organization-specific help services

Client Platform System Administrator (CPSA) Functions:

- Install initial User Application Software (UAS) and Operating Software (OS) upgrades
- Establish and assign Windows user-accounts
- Set privileges on the client host

- Establish Windows accounts on the Client host for users with administrative privilege
- Perform all software backups
- Secure backups
- Create data backups to support system recovery
- Perform system recovery involving installation of software as required by operating procedures

Client Platform System Security Officer (CPSO):

- Monitors and administers the client platform's security including audit data review, archiving, etc.
- Install IAVAs when directed
- Install anti virus software and updates as required
- Send AKP Archive audit data (OOB) to Client Service Node (CSN)
- Maintain PKI audit date IAW Type 1 Certificate Policy

Token System Security Officer (SSO):

- Maintains the SSO Password for each token
- Manages the SSO PINs for all tokens except their own
- Assists the user in unlocking token and uploading audit data from token to KMI
- Changes user's PIN

KMI Operating Agent (KOA):

- Enrolled by EM but does not need KOAM credentials to perform duties
- Designated by KOAM to access Primary Service Node (PRSN) Product Distribution Enclave (PDE) to retrieve encrypted products ordered for user devices assigned to KOA
- Designates registered users to be KOA for any KOA to which that manager is assigned

le Types	Role Names
ıal ıent roles	Ordering-and-distribution managers • Product Managers: – Controlling Authority – Command Authority • Product Requester • KOA Manager Registration managers • KOA Registration Manager • Personnel Registration Manager • Device Registration Manager • Personnel Local Type 1 Registration Authority • Device Local Type 1 Registration Authority Access control managers • Enrollment Manager User support managers • Service/Agency Help Desk Manager
ative ıent roles	Client Node administrators • Client Platform Administrator • Client Platform Security Officer
agement roles	Non-management users • KOA Agent

Description of KMI Roles

3.0 Assumptions

Development of a coherent training program is predicated on obtaining adequate data for its design and development. Training data must demonstrate test subjects can operate and maintain the equipment/system with minimal error.

Target audience for this system possess the Knowledge, Skills and Abilities (KSA) comparable to the level of complexity that is inherent in operating this system.

KMI CI-2 will utilize Training Aids, Devices, Simulators and Simulations (TADSS) where ever applicable to train individual and collective tasks. TADSS are an integral part of the training strategy and requirements are based on their use as presented in the strategy. Where applicable, training will be available in Interactive Multi-media Instruction (IMI) format as either Computer Based Training (CBT) in a stand-alone digital media format or as web-based training (WBT)hosted on either the Army Training Information Architecture (ATIA), Joint Learning Management System, or DoD Learning Management System. Courseware will comply with the most current version of the Sharable Content Object Reference Model (SCORM).

While it is probable, that fielding KMI CI-2 may cause a conversion in the Army S6/G6 Sections and IT/IA personnel, the level of this conversion has not been determined.

4.0 Training Constraints

For an undetermined period, it is possible that LCMS and KMI will be taught in parallel at the institution. This will incur the need for additional resources and instructors, both military and civilian to support the increased student throughput. To mitigate this, the school house has constructed two new MGC classrooms in addition to the existing LCMS classrooms.

No specific MOS is designated as "COMSEC Custodian," or "COMSEC Account Manager," (CAM). Therefore, unit commanders must be very selective in their choices regarding which personnel they send for training, as the schoolhouse cannot mandate who the units send, only that they meet the minimum requirements as stipulated in AR 380-40 and TB 380-40.

All KMI/MGC Training Support Packages (TSP) and IMI products are classified secret. This will place an additional burden on the school house to store all training materials in GSA approved containers at the end of each day. Open Storage will mitigate this effort and allow training materials and equipment to remain in the classroom without having to be locked in safes.

Institutional training is solely dependent upon facility/classroom readiness and availably of equipment, and the Key Management Infrastructure Training Storefront (KMITS), FUE for Spiral 2 is on or about 4QFY14. If it is projected that classrooms will not be ready by 4QFY14, PD NET-E and CIO G-6 will levy their option to shift MGC training to Tobyhanna Army Depot until such time the Cyber COE will have the classrooms ready for training.

5.0 System Training Concept

The KMI training concept will be developed in accordance with (IAW) One Army School System (OASS) guidance. Active Army (AA), Reserve Component (RC), and National Guard (NG) Soldiers will receive standardized, high-quality KMI training regardless of the component. Training will be implemented in three phases: New Equipment Training (NET), Unit Training, and Institutional Training as defined in TRADOC Regulation 350-70 Army Learning Policy and Systems, 6 Dec 11.

The Program Executive Officer (PEO), Project Manager (PM), and Materiel Developer (MATDEV), will collaborate with USACyber COE's TNGDEV to develop the STRAP, Training Support Packages (TSP), and Warfighter Training Support Packages (WTSP). Training materials will be developed in the Training Development Capability (TDC) database using the Analysis, Design, Development, Implementation, and Evaluation (ADDIE) process for all three training domains IAW TR 350-70.

MATDEV and TNGDEV will develop operator, maintainer, and Doctrine and Tactics Training (DTT) for institutional training. The doctrine and tactics training strategy provides training when required and feasible prior to NET/Displaced Equipment Training (DET), and it ends before sustainment training begins. This training is not part of a stand-alone strategy, but an integral part of the overall training strategy/package. DTT Team will provide training material to the new equipment training team (NETT) to field AA and RC units IAW AR 73-1 and DA PAM 73-1.

All digital training materials will be entered in and managed through the TDC database. This information drives embedded training and IMI product development for Distributed Learning (DL). Sharable Content Object Reference Model (SCORM) conformance is mandatory. IMI products will be loaded on the Army Learning Management System (ALMS). Individual and collective tasks updates will be used to update the Digital Training Management System and the Combined Arms Training Strategies (CATS). The TSPs will be modified to become the WTSPs with the addition of CATS. Final TSPs and WTSPs will be loaded on the Central Army Registry (CAR). These programs can be accessed via the Army Training Network (ATN).

5.1 New Equipment Training Concept (NET)

MATDEV will develop and conduct initial NET. Training methods, concepts, and technology will integrate instructor-led conferences with the use of Interactive Computer Based Training (ICBT), Interactive Courseware (ICW), IMI, and simulation modules whenever applicable. The MATDEV will plan, organize, fund, and field the NET effort IAW Army Regulation 350-1, Army Training and Leader Development. The USACyber COE & FG's DOT will approve all training requirements and plans. DL will be used wherever and whenever possible to leverage technologies in training to achieve the following benefits:

- Improved readiness
- Continuous training throughout the Soldier's career
- Closing gaps between training and operating environments
- Facilitating more responsive development and distribution of critical training
- Reduced Soldier's time away from unit/home
- Leveraging training efficiencies through multimedia and immersive training products
- Avoiding significant training cost
- Standardizing United States Army Reserve (USAR) , Army National Guard (ARNG) and Active Army (AA) training
- Placing publications and reference materials in digital form for quick use
- Accessibility to online education courses
- Quicker and wider dissemination of updated training materials
- More realistic simulations

Operator-maintainers, GPU, Staff Users/System Administrators (SU/SA), and network managers will use ICBT and IMI to install, initialize, operate, staff, manage, maintain, and configure KMI CI-2 components, platforms, terminals, and networks. NET will be conducted at Ft. Gordon, GA., Ft. Huachuca, AZ., the Professional Education Center (PEC), Little Rock, AR, Germany and Korea. The proponent institution will receive Instructor and Key Personnel Training (I&KPT) on or about 2QFY15. NET will be 80 hours.

MATDEV will assist training developers in acquiring the first production or procurement items and/or system particular support equipment, IAW Deputy Chief of Staff for Operations and Plans (DCSOPS) direction via the Distribution Plan, into the training base prior to other KMI CI-2 fieldings.

5.2 Displaced Equipment Training (DET)

Not Applicable

5.3 Doctrine and Tactics Training (DTT)

USACyber COE Combat Developer or TRADOC Capability Manager (TCM) will develop KMI CI-2 DTT. MATDEV will deliver DTT during NET.

5.4 Training Test Support Package (TTSP)

The TTSP being developed for KMI is the 80 hour MGC course curriculum.

6.0 Institutional Training Domain

Individual and collective tasks will be trained to AA and RC. AA and RC will receive the same training. RC training. Individual tasks will be taught at the institution and collective tasks are the responsibility of unit commanders. Institutional training will start in sufficient time to provide trained replacements for the first units equipped with the system. This will be on or about 1QFY15 but not later than one year after FUED unless the system fielding schedule justifies starting institutional training at a later date. This training is also dependent upon fielding of KMI CI-2 equipment, facility readiness, and the availability of the KMITS to the Cyber Center.

Additional institutions teaching KMI CI-2 will be Ft. Huachuca, AZ, Professional Education Center (PEC) at Little Rock, AR, Germany, and Korea.

6.1 Institutional Training Concept and Strategy

MATDEV or Product Director Net Enablers (PD NET-E) will provide training components (training materials, real equipment, simulations, simulators, etc.) to USACyber COE & FG along with NET materials and I&KPT materials IAW approved fielding plan. USACyber COE & FG will incorporate materials into the current 80 hour curriculum. The NET TSP will be used to establish the institutional training base. KMI CI-2 training materials will be available to develop NCO, WO, and Officer Key Management training courses. Every organization involved in the process of developing training products and services for KMI CI-2 must leverage current and emerging information-age technologies. MATDEV or system fielder, PD NET-E will provide I&KPT to USACyber COE & FG prior to institutional training being conducted.

6.1.1 Product Lines

The full complement of training support products required to support KMI CI-2 training constitutes the System TTSP. KMI CI-2 TTSP will provide the unit with a training package that supports NET.

6.1.1.1 Training Information Infrastructure

KMI CI-2 training material will conform to Joint and Army architectures and standards, and enable development, storage, retrieval, delivery, and management of training products. Training products will be planned, prepared, and developed IAW the following operational and technical architectures as applicable: Department of Defense Information Network (DODIN), ATIA, High Level Architecture (HLA) for simulations, and Common Training Instrumentation Architecture (CTIA). KMI CI-2 will leverage web-based technology to interface with the training infrastructure via the Tactical Internet (TI).

6.1.1.1.1 Hardware, Software, and Communications Systems

KMI clients are composed of three components: an Advanced Key Processor (AKP), key management software applications, and a computing platform. The AKP is successor to the EKMS KP, with similar functionality and form fit, enhanced performance, and a modular architecture.

Given varying needs of the KMI user community, KMI clients may need one or more key management applications based on needs of the specific user community. Examples of such applications would be modules to:

Support physical key products accounting

- Assist in ordering and managing modern key
- Assist in managing files containing downloaded encrypted keys
- Loading appropriate files into transfer devices for ECU loading

6.1.1.1.2 Storage, Retrieval, and Delivery

Digital information will be developed, maintained and stored on the MGC's Info-Center and on LandWarnet eUniversity (LWNeU), Battle Command Knowledge System (BCKS), Defense Connect Online (DCO), or other classified enabled military training repositories as necessary, and with new repositories as they evolve through the ATIA.

6.1.1.1.3 Management Capabilities

NET and institutional training programs will utilize the Army Learning Management System (ALMS) to track student progression through lessons, exercises, and evaluations. ALMS will be capable of downloading student academic records, tracking student progression, and sending the data back to LWNeU (https://lwn.army.mil/). Other services will utilize their appropriate management systems to track student progression.

6.1.1.1.4 Other Enabling Capabilities

KMI CI-2 to ECU Interface. KMI will supply multiple paths of communication to ECUs with various levels of automation and management capabilities. ECUs that are not KMI-Aware (a device that is known to KMI through registration, endorsement and initialization processes) will interface with CI-2 Client Nodes either directly or by transfer fill devices. Transfer fill devices are special-purpose devices that have a range of capabilities that can include storing, protecting and transferring protected, and unprotected key. The Client Node will be capable of reading from and writing to each of these fill devices. As new fill device technology becomes available, it is the intent for each Client Node to be able to interface with that new device in future capability increments. This interface will support functions that include key distribution, tracking, accounting, and auditing, etc.

System Nodes and Characteristics: The KMI initiative focuses on meeting key provisioning requirements of KMI and DODIN IA architecture by unifying dissimilar KM systems that exist today into a single, modern architecture one that is modular, flexible and extensible that will significantly reduce resources associated with operation, maintenance and training. This will be accomplished by transitioning from existing human key delivery and management systems to an automated Net-Centric KMI to ECU delivery and management system. The KMI development effort will expand upon current KM architectures by leveraging existing KM facilities and developing new solutions where needed. Major infrastructure nodes of the target KMI are the Central Services Node (CSN), Product Source Node (PSN), Primary Services Node (PRSN) and the KMI Client Node. KMI Client Node normally consists of both the KMI Client and the Advanced Key Processor (AKP). In some instances, the KMI Client will be deployed without an associated AKP. In these instances, the KMI Client without an AKP is still considered a KMI Client Node. The KMI Nodal view figure depicts the nodal view of the target KMI architecture and list services that are provided within each nodal enclave.

KMI CI-2 will consist of a number of nodes that provide a unified infrastructure for providing key management products and services, supporting a wide variety of users. In KMI, users are either consumers that depend on KMI for products and services or managers that allocate and control resources within KMI; customer organizations will typically have a mixture of users and managers. A logical configuration of KMI node types along with the functions allocated to each node type is shown below.

Client Service Node (CSN) - The CSN provides long-term system archive,

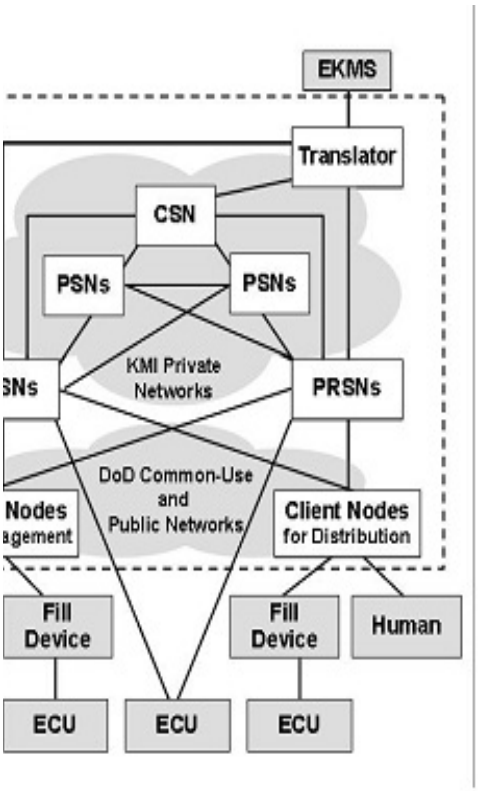
receives Intrusion Detection System (IDS) and audit data from the PRSNs for storage and archive.

Product Service Node (PSN) - PSNs generate and produce KM products at the request of the PRSNs.

Primary Service Node (PRSN) - KMI clients obtain KM products and services from a PRSN that provides common management functions in a server-based architecture across multiple classification domains. The PRSN provides unified and transparent access to KMI production sources and delivery of KMI products and services to consumers directly or through an intermediary.

Client Nodes - Also referred to as end entities, include stand-alone cryptographic devices, devices that incorporate security features that rely on KM services (e.g., security features within a router), and computing platforms using software applications that require KM support. Client Nodes cover a broad category of components and/or software applications that provide a user access to the products and services of KMI. The KMI Client Node normally consists of the KMI Client platform and the AKP. In instances where the KMI Client is deployed without an associated AKP, it is still considered the KMI Client Node. They can also take a variety of forms including security devices or embedded modules in enterprise systems. Clients can securely interface with the PRSN and allow users to perform management functions or request and receive products and services from KMI.

A logical configuration of the KMI node types along with the functions allocated to each node type is shown in the figure below:



System Nodes and Characterisics

6.1.1.2 Training Products

The follwoing training publications and products are being developed by the MATDEV for KMI:

An 80 hour training course

MGC Technical Manual

MGC Quick Reference Guide

CBTs will be developed in support of the following roles:

- Enrollment Manager
- Personnel Registration Manager
- Device Registration Manager
- KOA Registration Manager
- Command Authority
- Controlling Authority
- Product Requestor
- Token SSO
- Client Platform Administrator
- Client Platform Security Officer

6.1.1.2.1 Courseware

Courseware will consist of text-based help-style ICW and classroom based TSPs that will be integrated into KMI CI-2 institutional and unit training for the AA/USAR/ARNG as applicable. Electronic technical manuals (ETM) and electronic exportable TSPs will be used to augment delivery of ICW and CBT. The entire KMI MGC courseware is housed on the MGCs' Information Center, readily accessible to the student. These electronic manuals and TSPs can also be archived in the LWNeU portal, DKO-S, and the Defense Online (DCO) portals, provided they are secret enabled.

6.1.1.2.2 Courses

MATDEV will develop a Management Client (MGC) Operator's Course for managers, planners, and ACOM staff members planning KMI CI-2 acquisition and fielding.

This course provides instruction in Key Management Infrastructure architecture, Management Client (MGC), workstation hardware and related systems; system initialization and interface with other accounts; account for and manage COMSEC material; order, generate, and distribute traditional and modern keys; conduct inventories, destroy keys, and perform other accounting procedures; prepare and submit reports within the KMI hierarchy.

Training materials will include common core module and role specific modules. Role specific modules will enable the training course to be tailored to operational positions of students as determined during the training analysis. This strategy will allow students to receive only the training required to perform their job. Common core modules provide common information that is needed no matter what role the student will perform on the job. Modular development of common core materials supports multiple reuse. For example, all trainees will need common core modules such as Module A - System Overview and Module B - Node Description. However, only the LOA Registration Manager will need the role-specific module, Module F - KOA Manager. Modular development allows a variety of common core and role-specific lessons to be combined into a role-based/scenario-based curriculum.

Modular development will also simplify subsequent updates. Training materials for each spiral will build upon the training material submitted during the previous spiral. Twenty-eight modules were identified for development based on system roles for each node. Role-based/scenario-based operator training will be conducted using verified materials. It is anticipated that anywhere from 2 to 16 hours will be required to conduct training for any particular module.

PRSN/CSN Training. Users will require PRSN/CSN training to support testing. Users may attend multiple role-based modules depending on their job requirements and classroom capacity.

Help Desk and Infrastructure Support Training. The KMI CI-2 training team will train Help Desk Operators to ensure they have the knowledge to resolve

issues and to efficiently access and update information in their issues database. Training materials and technical manuals will remain readily accessible to Help Desk Operators to assist them in resolving caller issues. Materials used to conduct this training will be compiled into an exportable package for future use however, the bulk of Help Desk and Infrastructure training will be conducted via unit training.

MGC COURSES

Conduct System Overview

Define Information Assurance

Define Key Management Infrastructure (KMI) Roles

Define Key Management Infrastructure (KMI) Responsibilities

Establish Platform User Account

Install System Software

Establish MGC User Account

Maintain System Configuration

Manage Network Connectivity

Monitoring Platform Security

Audit Data Management

Manage System Reports

Establish New Product Requirements

Generate Crypto Product Request

Manage Account Distribution Profile (ADP)

Destroy Crypto Product

Establish New Product Requirements

Manage Account Distribution Profile (ADP)

Generate Crypto Product Request

Modify Account Distribution Profile (ADP)

Identify KOA Enrollment Request

Manage KOA Agent Request

Inventory KMI Operating Account (KOA)

De-register KMI Operating Account

Order KMI Aware Device

Issue Key for Management Client Device

Manage Device Distribution Profile

Process Key Accountable Product

Transfer Accountable Product

Issue Crypto Product

Import KOA Key

Generate Local Key

Destroy Crypto Product

Inventory KOA

Initialize KMI Aware Device

De-register KMI Aware Device

Modify KMI Manager Registration

De-register KMI Manager

Perform Token Personalization

Initiate Product Delivery

Enable Enclave (PDE)

Endorse KMI Device

Process Non PDE

Enabled KMI Aware Device Endorsement

Register KOA

Synchronize Short Title Profile

Distribute information between EKMS and KMI

Process KMI Agent Enrollment

Retrieve Key Product

Relocate KMI Operating Account

Backup KMI Operating Account

6.1.1.2.3 Training Publications

PD NET-E will develop the Integrated Operator/Maintenance Manual. All training materials, TMs and publications will be resident on the Management Client's (MGC) info center.

6.1.1.2.4 Training Support Package (TSP)

MATDEV will develop a series of scenario based TSPs. TSPs will be designed to support effective KMI CI-2 operator training. TSPs will make maximum use of DL technology. As appropriate, TSPs will be IMI structured programs presented on a computer-based system. If applicable, courseware will be delivered in two versions. One version of the courseware will be delivered over Secure Internet that is playable in either the Microsoft Internet Explorer browsers versions 5.x or higher, or the Mozilla Firefox browser versions 5.x or higher. The second version will be a stand-alone mode, delivered via CD-ROM/Digital Video Disc (DVD). The KMI CI-2 TSP must train core tasks; develop proficient Soldiers, leaders, staff and units; and support AA/RC personnel. MATDEV will plan, program, and budget for TADSS that are required to support the training of KMI CI-2.

6.1.1.3 TADSS

Training Aids, Devices, Simulations and Simulators (TADSS) will be an additional source to train KMI CI-2. TADSS developed must be multifunctional and support training for all affected AFSCs, MOSs, NECs, AOCs, and FAs. TADSS should include Levels 2 through 4 interactivity, TM based, easily replicated, non-proprietary, and proceeds through the following process: acquire, familiarize, practice, and validate. An exception to this requirement will be those Service specific components having special instructional delivery needs that exclude TADSS. All KMI CI-2 institutional training requiring TADSS will adhere to the Joint Standards for TADSS. If Joint Standards do not exist, the TADSS will adhere to the practices and guidelines of the Executive Agent with input from the other Service components. Service components will identify their individual TADSS if needed. Designs for simulations should include simulation software residing on the users PC platform and have the capability to use multiple simulation applications on the same platform. Platform screen will display icons such as a photo of the system for various simulations. User will select appropriate icon, load program, and use simulation to execute their training where ever applicable.

TADSS developed for KMI CI-2 shall provide students an easy to use human system interface, courseware loading and playability process, and course navigation. PM must ensure CBT for the system training suites has the capability to monitor and assess the efficiency and effectiveness of system performance task training. The software system must be capable of initiating, maintaining, and downloading student records when used at the institution. Training software will be capable of securing student record data.

6.1.1.3.1 Training Aids

MATDEV will develop CBTs and WBT for supporting the KMI CI-2 environment during NET and Soldier Unit Sustainment Training. A Sharable Content Object Reference Model (SCORM) version 2004, version 3 compliant. It will accurately present system operation for user self-study and practice. CBT/WBT will be developed in a modular format based on the operational tasks for each user role. It will provide visual demonstrations of system operations (show me) and a realistic way to practice system tasks without affecting the actual system (try it).

CBT/WBT shall provide students an easy to use human system interface, courseware loading and playability process, and course navigation. PM must ensure CBT for system training suites has the capability to monitor and assess efficiency and effectiveness of system performance task training. The software system must be capable of initiating, maintaining, and downloading student records when used at the institution. Training software will be capable of securing student record data.

CBT/WBT will contain learning checks to provide students with realistic practice opportunities to evaluate their performance. A printable certificate will verify student proficiency in each critical performance area. Upon successful completion of self-learning checks for each critical performance area, students will be able to print a job aid to use in performing actual system operations. The CBT will be supportable in both a stand-alone and a web-accessible format.

The following CBTs will be developed in support of the following roles:

- Enrollment Manager
- Personnel Registration Manager
- Device Registration Manager
- KOA Registration Manager
- Command Authority
- Controlling Authority
- Product Requestor
- Token SSO
- Client Platform Administrator
- Client Platform Security Officer

6.1.1.3.2 Training Devices

Not Applicable

6.1.1.3.3 Simulators

Not Applicable

6.1.1.3.4 Simulations

Software simulations and ICBT will be developed for KMI CI-2 institutional training. These training products will deliver critical KMI CI-2 knowledge and skills for the installer, operator-maintainer, SU, SA, network planner, and network manager. CBT will be integrated into the Client user interface. It will be delivered as part of the CI-2 system. CBT with additional roles will also be available as a leave-behind/sustainment training package.

6.1.1.3.5 Instrumentation

Not Applicable

6.1.1.4 Training Facilities and Land

Two additional CONUS KMI training facilities will be stood up. The first one will be at Ft. Huachuca, AZ. Once NET is complete, that suite of equipment will be transferred to USACyber COE to equip one of its classrooms. The second KMI training facility is the Professional Education Center (PEC), at Little Rock, AK.

6.1.1.4.1 Ranges

Not Applicable

6.1.1.4.2 Maneuver Training Areas (MTA)

Not Applicable

6.1.1.4.3 Classrooms

Two additional KMI training facilities will be stood up. The first one will be at Ft. Huachuca, AZ, after which, when NET is complete, that suite of equipment will be transferred to USACyber COE to equip one if its classrooms. The second KMI training facility being considered is the Professional Education Center (PEC), at Little Rock, AK.

6.1.1.4.4 CTCs

Not Applicable

6.1.1.4.5 Logistics Support Areas

Communications Security Logistics Activity (CSLA) will provide all logistical processing, support, storage and staging for accounts transitioning from AKMS/EKMS to KMI. The Army Customer Support Center at CSLA will provide KMI help desk service to the Army. The CSLA Help Desk will serve as the Army's face to the field and provide assistance and advice/guidance regarding KMI client node software, hardware and operations to Army KMI users. Selected CSLA personnel will also support various KMI infrastructure roles as a representative of the Army Service Authority (ASA). CSLA will also provide item management of the MGC and its major components.

Tobyhanna Army Depot (TYAD). Tobyhanna Army Depot (TYAD) will provide both fielding and depot support functions with respect to Army client nodes. TYAD will ensure strict enforcement of accounting policies and procedures, proper handling and storage, and access control during its operation, shipment, maintenance, or repair, until final disposition of Controlled Crypographic Item (CCI) at TYAD.

Other agencies providing additional support for KMI are the Product Director Network Enablers (PD NET-E), Communications-Electronics Research Development and Engineering Center (CERDEC).

6.1.1.4.6 Battle Command Training Centers (BCTC)

No BCTCs have been identified for KMI CI-2 institutional training.

6.1.1.5 Training Services

KMI will require training services to enable sustainment training in all the training domains. Sustainment includes updates to publications and technical manuals, as well as changes to the training products that support KMI in all training domains. These services will support life cycle management of training materials and products that are used to train Warfighters as KMI hardware, operational environment and software are updated and changed.

6.1.1.5.1 Management Support Services

USACyber COE Directorate of Training (DOT), along with TRADOC Capability Manager for Networks and Services (TCM-N&S) will be responsible for implementing management support services in support of KMI. These life cycle management services will support changes and updates to training materials and products across the training domains. As new requirements and technology emerges, there will in turn be hardware and software updates to KMI. TCM-N&S will manage emerging capabilities, requirements and technology, while DOT manages the changes to training materials and products as a result of these upgrades to KMI.

6.1.1.5.2 Acquisition Support Services

TNGDEV, in conjunction with Combat Developer (CBTDEV) and Materiel Developer (MATDEV), will explore best possible options for contracting development of KMI training products. This includes correctly conveying the KMI training strategy to the MATDEV. The MATDEV should be able to deduce from the training strategy the types of training products needed for each domain to support KMI training.

6.1.1.5.3 General Support Services

KMI client node training will be accomplished by a combination of on-the-job training, computer based media and institutional training. NSA in the role of KMI PMO has undertaken establishment of a Joint Service Training Working Group to monitor and assist the vendor with development and modification of the MGC training package. Spiral 1 training package has been developed and will support both IOT&E and Spiral 1 NET.

During the Spiral 2 development process, the training package will be updated with each capability spin delivery. All Services will implement and use the same MGC core training package for NET as well as subsequently employ the same package in support of Service institutional training. Projected course length is eighty (80) hours.

6.1.2 Architectures and Standards Component

Not Applicable

6.1.3 Management, Evaluation, and Resource (MER) Processes Component

TBD

6.1.3.1 Management

Directorate of Training (DOT) and Capabilities, Development and Integration Division (CDID), in close coordination with TRADOC Capability Manager for Networks & Services (TCM-N&S), will manage KMI effort as the Training Developer and Combat Developer, respectively. Embedded in the DOT are training specialists/developers, charged with ensuring all aspects of training are identified and implemented. Both organizations will participate in strategy development with regards to tactical operations and training. Both organizations will monitor, comment on, and attend concept development and experimentation meetings dealing with KMI. Training requirements will be developed and incorporated in requirements documents and the System Training Plan (STRAP) developed and updated as required by the Joint Capabilities Integration and Development System (JCIDS).

6.1.3.1.1 Strategic Planning

TRADOC is defining methods to train Army XXI. ATXXI is the Army's training strategy to ensure that Army XXI realizes its potential through battle-focused training using state-of-the-art training support capabilities. It is a modernization effort that encompasses three Force XXI axes through, collective, individual, and systems training. The ATXXI Campaign Plan implements ATXXI training strategy using three training axes: Warfighter XXI, Warrior XXI, and Warfighter Modernization (WarMod) XXI. These axes support unit, institutional (including distributed learning (DL) and self development), and Army modernization training (AMT). They are interdependent and mutually supporting. The axes rely heavily on information technology to support modernized classrooms, DL, training development (TD), testing, and training management. TRADOC will ensure meeting the Army's requirement for tough, realistic training by using Force XXI Information Age Technologies and a mix of virtual, constructive, gaming and live training environments. One of the Army's top priorities is "digitizing the battlefield" to provide seamless digital command and control capabilities throughout the fighting force. Multiple initiatives are underway to harness microprocessor and information technology to maintain an edge in projecting and employing power on future battlefields and to embed complex, combined arms, structured training into the digitized force. The technologies cover a wide range, from simple conversion of text to digital formats in Synthetic Environments with high fidelity digital representations of actual terrain.

6.1.3.1.2 Concept Development and Experimentation (CD&E)

Proponents use the Training Development Capability (TDC) to develop collective (Warfighter), individual (Warrior), and AMT (WarMod) training products. With implementation of the Total Army School System (TASS), Reserve Components (RC) are taking a proactive role in the analysis, design, development, and validation of One Army School System (OASS) Courses. Training development of KMI training products must be more responsive and take less development time. Current and future automation tools which comprise the current TD automation system, TDC, will assist in training analysis, design, and development. Training development must also satisfy future training requirements by applying information-age technologies instead of relying on instructor-led instruction and utilize Warfighter Rapid Acquisition to maximize resources. Training developer involvement in Advanced Warfighter Experiments will involve spiral development of training products in an environment that allows one to test, fix, and test again to gain new insights into the effects of training as it is developed rather than waiting until the "end" to evaluate and implement changes. Development is accelerated through experiential learning and documentation. Insights gained through experiences provide input to the development of training products and processes. Experiences begin with the simple, and move through the complex. Each experience captures new information that is applied to the following exercise or products. The entire process is planned to permit spiral development and training to the next level. Using the automated tools available to training developers (specifically TDC and its related CATS and doctrine components) allows for a faster and more efficient development process. KMI training products must support the live, virtual, constructive and gaming (LVCG) training environments.

6.1.3.1.3 Research and Studies

Not Applicable

6.1.3.1.4 Policy and Guidance

The following documents provide guidance and direction for the TSS:

- AR 350-1 and AR 350-38
- TRADOC Regulations 350-70 and 71-20
- TRADOC Pamphlet 71-20

6.1.3.1.5 Requirements Generation

This STRAP supports the Key Management Infrastructure (KMI) Capability Increment 2 (CI-2) Capability Production Document.

6.1.3.1.6 Synchronization

Existing training POIs and courses already in place will need to be updated to not only include the Cyber COE, but also satellite schools that will prepare to train KMI. KMI training materials and products will also need to be incorporated and synchronized with LandWarNet e-University DL courses as well. Training materials must also be synchronized with Operational and Self-Development Domains.

6.1.3.1.7 Joint Training Support

A systems approach will be used for creating an Inter-service common core KMI curriculum. Each Service/NSA reserves the right to repackage the curriculum to meet the Service's/NSAs requirements, as long as, the common core curriculum is presented and the common assessment of student proficiency is administered and scored consistently with a passing score threshold of 75% enforced. The overall security classification of the KMI training program within each respective Service schoolhouse will be classified SECRET//Releasable to USA, AUS, CAN, GBR, and NZL. Course control documents (training plan, training standard, course chart, POI, practical exercises, etc.) will be Unclassified; so to not disrupt the approval process for obtaining funding, manpower, and resources of the Services schoolhouse. The lesson plan will be classified SECRET, commensurate with the training program. The common core KMI curriculum will not exceed 80 classroom hours; any Service's/Civil Agency's KMI policy training will be an adjunct to the 80 classroom hours.

Life-cycle Software/Training Support. NSA PMO will provide life-cycle sustainment for software and training development for the life of the KMI program post IOT&E.

6.1.3.2 Evaluation

KMI training in all training domains must be evaluated to ensure our Soldiers receive effective and up to date training. Evaluation of KMI training and training materials and products will provide the feedback needed to make modifications and adjustments to training materials, products, facilities, delivery methods and classroom sizes. KMI training evaluation will employ a variety of techniques. The following evaluation methods will be used at a minimum: Quality Assurance (QA), Assessments, Customer Critiques and Feedback, Lessons Learned, and After Action Reviews (AAR).

6.1.3.2.1 Quality Assurance (QA)

The proponent Quality Assurance Office (QAO) will use proven techniques to determine the quality of training provided by the institution. Internal evaluations will focus on presentation of the tasks at the institution, course content, and instructor presentation of material. QAO will be responsible for conducting any Post Fielding Training Effectiveness Analysis (PFTEA). Observations will be reported to the DOT for corrective actions.

6.1.3.2.2 Assessments

QAO conducts assistance visits with selected units and organizations. They provide spot-checks and assign an assessment ratings of "Met", "Met with Comment", "Not Met", or "Higher Headquarters Issue (HHI)"for each area. QAO gives specific attention to all areas TRADOC rated as anything other than "Met". For courses that are not reviewed by TRADOC, QAO conducts a thorough review of the checklists and supporting documentation. Applicable key leaders receive feedback via a formal out brief and/or a written assessment in the Sustain/Improve/Develop format used by the TRADOC evaluation team.

6.1.3.2.3 Customer Feedback

The Warfighters we train are our greatest feedback source for conducting internal quality assurance of training. The student critique process is a great assessment tool for evaluating the effectiveness of the TSS and can be used to make necessary adjustments to training products, classroom size, and POI/lesson plans. The goal of the feedback process is for course managers and senior instructors to incorporate student opinions in the overall training evaluation process.

6.1.3.2.4 Lessons Learned/After-Action Reviews (AARs)

The Army Lessons Learned Library can and will serve as a valuable resource for Soldiers to improve their skills at operating and deploying KMI training products and materials as well as serve to make corrections and updates to training products and material.

6.1.3.3 Resource

The Capability Production Document (CPD) specifies training is properly resourced by the Program Objective Memorandum (POM) briefing presented by the MATDEV (PM). Resources provided by the PM would include any training Aids, Devices, Simulations, as identified in the requirements document.

1. Training Developers (TNGDEV)

Item Resourced	Prior	FY14 Yrs or $K	FY15 Yrs or $K	FY16 Yrs or $K	FY17 Yrs or $K	FY18 Yrs or $K	FY19 Yrs or $K
Manpower - TD							
Contractor		$400K	$500K	$500K	$500K	$500K	$500K
Civilian		$300K	$500K	$500K	$500K	$500K	$500K
Enlisted			$200K	$200K	$200K	200K	$200K
Warrant							
Officer							

Contract/Spt		$300K	$300K	$300K	$300K	$300K	$300K
Civ Pay		$400K	$400K	$400K	$400K	$400K	$400K
Trvl/Per Diem		$50K	$75K	$75K	$75K	$75K	$75K
Other		$40K	$40K	$40K	$40K	$40k	$40K

Rationale: TNGDEVs are needed to develop and maintain the programs of instruction and other outputs of the SAT process. Military personnel will be used in different areas within the training program. Travel/Per Diem represents cost to attend training and reviews; and four instructor/key personnel to evaluate training prior to operational testing.

2.) Training Products

Item Resourced	Prior Yrs or $K	FY14 Yrs or $K	FY15 Yrs or $K	FY16 Yrs or $K	FY17 Yrs or $K	FY18 Yrs or $K	FY19 Yrs or $K
Training Products							

Training Pubs		$200K	$200K	$200K	$200K	$200K	$200K
TSP		$150K	$150K	$150K	$150K	$150K	$150K
IMI		$250K	$250K	$250K	$250K	$250K	$250K
ETM		$200K	$200K	$200K	$200K	$200K	$200K
STP							
IETM		$40K	$40K	$40K	$45K	$50K	$50K
CATS		$100K	$100K	$100K	$100K	$100K	$100K
Printing		$5K	$5K	$5K	$5K	$5K	$5K
Distribution		$1K	$1K	$1K	$1K	$1K	$1K
Other		$5K	$5K	$5K	$5K	$5K	$5K

Rationale: Cost to develop, revise, maintain, and distribute Training Products. Includes cost to develop TSP that will be used for NET,

institutional, operational, and self-development domains.

3.) TADSS

Item Resourced	Prior	FY14 Yrs or $K	FY15 Yrs or $K	FY16 Yrs or $K	FY17 Yrs or $K	FY18 Yrs or $K	FY19 Yrs or $K
TADSS							
Simulators							
Simulations							
GTA							
Software		$0K	$0K	$5K	$5K	$5K	$5K
Trng Equip*		$0K	$0K	$912K	$912K	$0K	$0K
Equipment		$785K	$260K	$10K	$10K	$10K	$10K
Printing		$0K	$0K	$10K	$10K	$10K	$10K

Shipment		$70K	$35K	$1K	$1K	$1K	$1K
Sustainment		$0K	$0K	$5K	$5K	$5K	$5K
Other							

Rationale: Includes the cost to procure and maintain actual systems for training use. Forty six (46) actual operational systems are required for use as training devices.*Actual item of equipment used for training which does not lose its identity as an end item for operational purposes.

4.) Facilities

Item Resourced	Prior	FY14 Yrs or $K	FY15 Yrs or $K	FY16 Yrs or $K	FY17 Yrs or $K	FY18 Yrs or $K	FY19 Yrs or $K
Facilities/Land							
Facilities		$100K	$50K	$50K	$10K	$10K	$10K
Land		$0	$0	$0	$0	$0	$0

Site Surveys		$1K	$1K	$0K	$0K	$0K	$0K
AC/DC Power		$10K	$10K	$10K	$10K	$10K	$10K
Equipment		$785K	$20K	$20K	$20K	$20K	$20K
Maintenance		$10K	$10K	$10K	$10K	$10K	$10K
Other		$150K	$150K	$10K	$7K	$7K	$7K

Rationale: Cost to modify existing facilities to accommodate new power and shielding requirements of new system and electrical power needed to operate equipment.

5.) Software License and IT Support

Item Resourced	Prior	FY14 Yrs or $K	FY15 Yrs or $K	FY16 Yrs or $K	FY17 Yrs or $K	FY18 Yrs or $K	FY19 Yrs or $K

Training Services/TII							
LMS		$6K	$6K	$8K	$7K	$6K	$5K
Services		$1K	$1K	$1K	$1K	$1K	$1K
Servers		$1K	$1K	$1K	$1K	$1K	$1K
Licenses		$1K	$1K	$1K	$1K	$1K	$1K
IT Support		$5K	$5K	$5K	$5K	$5K	$5K
Other		$0.5K	$0.5K	$0.5K	$0.5K	$0.5K	$0.5K

Rationale: Software license and IT support will be required.

7.0 Operational Training Domain

KMI CI-2 operational training objective is unit and individual/crew combat readiness, the development of lethal teams, Soldiers, and Leaders. Field commanders continue to employ the principles of Army training to train mission-essential tasks at the unit-level. Unit training will be hands-on and standards based. The intent is to provide Leaders, units, and Soldiers with a realistic, operationally relevant training environment that replicates the full spectrum of wartime operations. It will also allow the command to integrate KMI CI-2 across Warfighting Functions.

Operational training requirements for KMI CI-2 will be integrated into all affected units CATS which are the unit training strategy for current and future training and identifies, quantifies and justifies the training resources required to execute training. The goal of operational training is to sustain individual, leader, battle staff and collective proficiency. Commanders are responsible for planning, resourcing and executing unit training which is based on CATS which provide commanders with a training framework. Training developers and commanders need to ensure any new operational training requirements to sustain unit training are integrated into existing unit CATS which provides the linkages from capabilities to collective tasks and provides a gated strategy using the crawl-walk-run approach to training. Integrated CATS supports training events/exercises and frequencies, identifies resources and training support requirements, and recommends multi-echelon training opportunities.

7.1 Operational Training Concept and Strategy

Units fielded KMI CI-2 will be able to practice individual and collective tasks using the system in a static training environment. Unit training will be conducted initially through NET when KMI CI-2 is fielded. All NET materials will be provided to the unit so that the unit can develop its sustainment training program. Units will incorporate training requirements into scheduled CATS training events such as field training exercises (FTX), and similar exercises.

7.1.1 Product Lines

Individual and collective/crew tasks will be trained to both the AA/RC. There will be no difference in training content between AA/RC. Tasks will be developed in TDC so they can be delivered to the Soldiers in the operating force through the Digital Training Management System (DTMS).

7.1.1.1 Training Information Infrastructure

See Paragraph 6.1.1.1

7.1.1.1.1 Hardware, Software, and Communications Systems

See Paragraph 6.1.1.1.1

7.1.1.1.2 Storage, Retrieval, and Delivery

Individual and collective training products will be developed in accordance with TRADOC Regulation 350-70 and designed through TDC so they can be delivered to the operational forces through the DTMS.

7.1.1.1.3 Management Capabilities

DTMS is the primary means for managing and delivering training products, (Collective Tasks, Individual Tasks Drills, CATS) to the operating force. AR 350-1 Chapter 4, directs that DTMS is the primary authorized automated system for managing training in Army units.

7.1.1.1.4 Other Enabling Capabilities

See Paragraph 6.1.1.1.4

7.1.1.2 Training Products

Training products associated with Operational Training are centered on those items utilized during NET and institutional training - i.e. simulations and simulator use, and DL. These training products, will be delivered with the NET TSP during the Unit NET. Operational training will be accomplished with the NET TSP, including any CBTs and IMI to be left with the unit following NET.

7.1.1.2.1 Courseware

Courseware will consist of text-based help-style ICW and classroom based TSPs that will be integrated into KMI CI-2 institutional and unit training for the AA/RC as applicable. Electronic technical manuals (ETM) and electronic exportable TSPs will be used to augment delivery of ICW and CBTs. These electronic manuals and TSPs can be archived in the LWNeU portal, the Central Army Registry (CAR), and the Defense Connect Online (DCO) portals.

7.1.1.2.2 Courses

No formal courses will be provided that specifically focus on operational training, other than those courses taught during NET and institutional training. The institutional courses are developed in such a way that commanders can add the training objectives to unit missions trained in both field and garrison environments.

7.1.1.2.3 Training Publications

All training materials, publications and user manuals will be available on the MGCs information center in digital format.

7.1.1.2.4 TSP

See Paragraph 6.1.1.2.4

7.1.1.3 TADSS

See Para 6.1.1.3

7.1.1.3.1 Training Aids

See Paragraph 6.1.1.3.1

7.1.1.3.2 Training Devices

Not Applicable

7.1.1.3.3 Simulators

Not Applicable

7.1.1.3.4 Simulations

See para 6.1.1.3.4

7.1.1.3.5 Instrumentation

During scheduled test events, developmental test facilities were made available to Service/Agency operational test personnel for early familiarity and informal training. Developmental Test Organization (DTO) personnel will perform Spiral 1 and Spiral 2 System DT&E2 at Test Infrastructure (TI) facilities, utilizing network resources and operationally representative test key material and system components. This test event will utilize KMI systems that are configured for use in a test environment but are destined to be used for the operational mission. Further, this test event will use operationally representative test data and key material. The test sites and facilities identified for participation in System DT&E2 for each KMI spiral will include utilization of the NSA EKMS TI and the KMI TI. The test sites and facilities identified for participation in Operational Assessment 1 (OA1) and OA2 events for each KMI spiral will include utilization of the KMI TI. Appropriate KMI system components will interface with the EKMS TI to result in a KMI TI that mirrors the operational environment. Spiral 1 OA1 will use the same test environment as System DT&E2.

7.1.1.4 Training Facilities and Land

See Para 6.1.1.4

7.1.1.4.1 Ranges

Not Applicable

7.1.1.4.2 Maneuver Training Areas (MTA)

Not Applicable

7.1.1.4.3 Classrooms

see Para 6.1.1.4.3

7.1.1.4.4 CTCs

KMI CI-2 will interface with communication components of Combat Training Center-Instrumentation Systems (CTC-IS). The CTC-IS will be used to validate the ability of units to employ KMI CI-2 within the force.

7.1.1.4.5 Logistics Support Areas

Maintenance for fielded Army operational Client Nodes will be managed through the Army Customer Support Center. The Army Customer Support Center is located at Fort Huachuca, Arizona and operates Monday through Friday 0600 to 1700 MST. Virtual service is provided after hours and on weekends and holidays for emergency situations. E-mail requests can also be sent to tier2cst@conus.army.mil . The support center can be contacted toll-free at 877-896-8094 or DSN 879-9900. The NSA and Service help desks will leverage a single integrated Help Desk trouble ticket system which will provide real time access to trouble history data and troubleshooting decision charts. The integrated ticket system will also provide metrics support to assist in the identification of systematic KMI problems or potential KMI supportability issues.

Field Level maintenance involves preventive maintenance, fault isolation, limited software recovery actions, and replacement of faulty LRUs. The KMI user will receive introductory training to support the setup, operation, and maintenance of the KMI Client Node IAW the published procedures of the MGC Operator Maintenance Manual (OMM). The Customer Support Center will serve as the first level of support for all Army Client Nodes, client operator personnel, and the supported KOA accounts. The KMI operators will perform preventative and limited maintenance and assist with fault isolation under the direction of customer support technicians . Issues that cannot be resolved will be referred by the Army Customer Support Center to the NSA KMI Help Desk. Once hardware issues are diagnosed, customer support personnel and/or the item manager will provide guidance to the user regarding the disposition of the failed Lowest Replaceable Unit (LRU). The replacement LRU will be sent to the client user from the FSP, depot, or a designated operational backup site. Army users will send failed parts to the Army depot for first look and disposition. The Army depot will backfill the FSP; and the PICA will backfill the Army depot.

Customer Service Support
The Army Customer Support Center will work closely with other Service Help Desks and the NSA KMI Help Desk to provide detailed troubleshooting history in a single integrated Help Desk trouble ticket database available on the SIPRNET. Army service technicians will have the ability to access composite maintenance history to better support solution selection, user direction, and alternative corrective actions. The Hewlett-Packard Service Manager (HPSM) has been selected as the tool to support the DoD wide information

collection effort. HPSM will additionally provide the metrics to analyze trends, evaluate supportability issues, and highlight specific problem areas.

Depot Maintenance and Sustainment
Sustainment Level maintenance will consist of fault isolation, parts and supplies support, and license and warranty actions, as required. The Air Force's Cryptographic System Division (CPSD) has been selected as the PICA Depot/Defense Maintenance Activity (DMA) for KMI including the KMI Client Nodes. Subsequent to the Army's first look, all reparable equipment and LRUs will be shipped to the KMI PICA for repair. Non-repariable equipment will be returned to the sparing pool for final disposition. The KMI DMA will provide services IAW standard PICA requirements. The Army depot is the PICA for the KG-250. An abbreviated list of PICA services follows.

Verify suspect LRUs
Provide repair estimates
Execute spare replenishment
Maintain database and trend analysis
Repair AKPs
Facilitate the repair of COTS equipment
Complete LRU destruction and/or distribution actions

7.1.1.4.6 Battle Command Training Centers (BCTC)

Not Applicable

7.1.1.5 Training Services

See para 6.1.1.5

7.1.1.5.1 Management Support Services

See Para 6.1.1.5.1

7.1.1.5.2 Acquisition Support Services

See Para 6.1.1.5.2

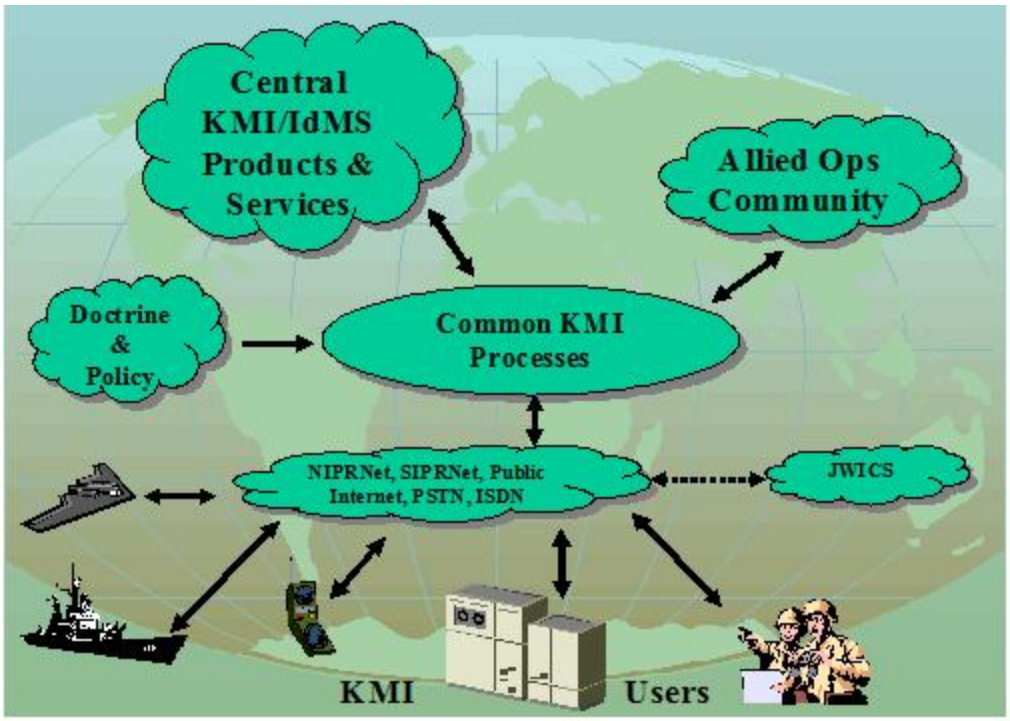
7.1.1.5.3 General Support Services

See para 7.1.1.5.3

7.1.2 Architectures and Standards Component

7.1.2.1 Operational View (OV)

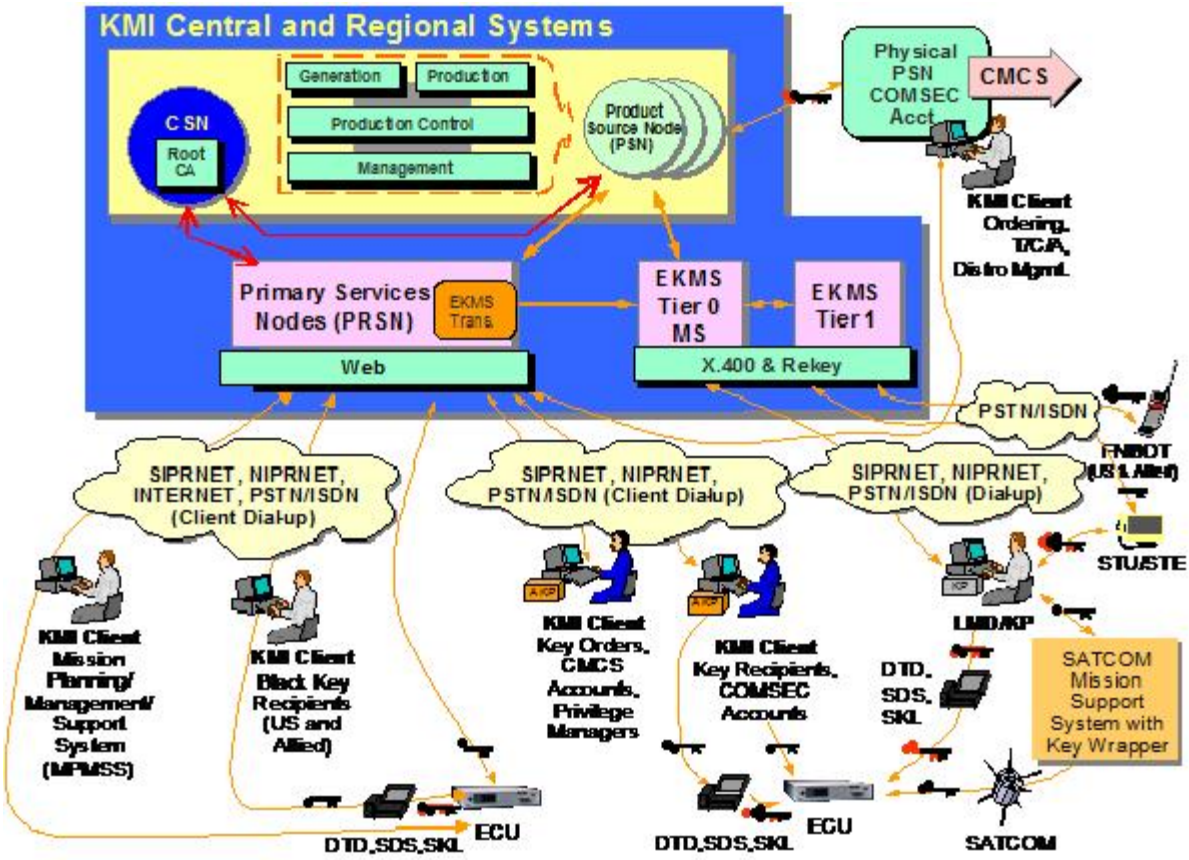
Army transformation is grounded in the operational framework of joint doctrine and concepts for future, joint and combined operations. Joint force commanders require Army elements to be able to conduct any mission assigned in the context of rapid decisive operations. This infrastructure will provide a means for the secure generation, production, distribution, management and auditing of cryptographic products.



KMI Operational View

7.1.2.2 Systems View (SV)

KMI CI-2 and its components shall be based on an open system architecture design and implement standardized interfaces to allow integration with other system components.


KMI Central and Regional Systems
Generation
Production
Production Control
Management
CSN
Root CA
Product Source Node (PSN)
Physical PSN COMSEC Acct
CMCS
KMI Client Ordering, TA, Distro Mgmt.
Primary Services Nodes (PRSN)
EKMS Trans
EKMS Tier 0 MS
EKMS Tier 1
Web
X.400 & Rekey
PSTN/ISDN
FNBDT (US & Allied)
STU/STE
SIPRNET, NIPRNET, INTERNET, PSTN/ISDN (Client Dialup)
SIPRNET, NIPRNET, PSTN/ISDN (Client Dialup)
SIPRNET, NIPRNET, PSTN/ISDN (Dialup)
LMD/KP
KMI Client Mission Planning/ Management/ Support System (MPMSS)
KMI Client Black Key Recipients (US and Allied)
KMI Client Key Orders, CMCS Accounts, Privilege Managers
KMI Client Key Recipients, COMSEC Accounts
DTD, SDS, SKL
SATCOM Mission Support System with Key Wrapper
DTD,SDS,SKL
ECU
DTD,SDS,SKL
ECU
SATCOM

7.1.2.3 Technical View (TV)

Not Applicable

7.1.3 Management, Evaluation, and Resource (MER) Processes Component

See para 6.1.3

7.1.3.1 Management

See Para 7.1.3.1

7.1.3.1.1 Strategic Planning

See Para 6.1.3.1.1

7.1.3.1.2 Concept Development and Experimentation (CD&E)

See para 6.1.3.1.2

7.1.3.1.3 Research and Studies

See Para 6.1.3.1.3

7.1.3.1.4 Policy and Guidance

See para 6.1.3.1.4

7.1.3.1.5 Requirements Generation

Not Applicable

7.1.3.1.6 Synchronization

Refer to Para 6.1.3.1.6

7.1.3.1.7 Joint Training Support

Refer to Para 6.1.3.1.7

7.1.3.2 Evaluation

Refer to Para 6.1.3.2

7.1.3.2.1 Quality Assurance (QA)

Refer to Para 6.1.3.2.1

7.1.3.2.2 Assessments

Refer to Para 6.1.3.2.2

7.1.3.2.3 Customer Feedback

Refer to Para 6.1.3.2.3

7.1.3.2.4 Lessons Learned/After-Action Reviews (AARs)

Refer to Para 6.1.3.2.4

7.1.3.3 Resource Processes

Training Products

Item Resourced	Prior Yrs or $K	FY14 Yrs or $K	FY15 Yrs or $K	FY16 Yrs or $K	FY17 Yrs or $K	FY18 Yrs or $K	FY19 Yrs or $K
Training Products							
Training Pubs		$200K	$200K	$200K	$200K	$200K	$200K
TSP		$150K	$150K	$150K	$150K	$150K	$150K
IMI		$250K	$250K	$250K	$250K	$250K	$250K
ETM		$200K	$200K	$200K	$200K	$200K	$200K
STP							
IETM		$40K	$40K	$40K	$45K	$50K	$50K
CATS		$100K	$100K	$100K	$100K	$100K	$100K

Printing		$5K	$5K	$5K	$5K	$5K	$5K
Distribution		$1K	$1K	$1K	$1K	$1K	$1K
Other		$5K	$5K	$5K	$5K	$5K	$5K

Rationale: Cost to develop, revise, maintain, and distribute Training Products. Includes cost to develop TSP that will be used for NET, institutional, operational, and self-development domains.

Item Resourced	Prior	FY10 Yrs or $K	FY11 Yrs or $K	FY12 Yrs or $K	FY13 Yrs or $K	FY14 Yrs or $K	FY15 Yrs or $K
Manpower - TD							
Contractor							
Civilian							
Enlisted							

Warrant							
Officer							
Contract/Spt							
Civ Pay							
Trvl/Per Diem							
Other							

8.0 Self-Development Training Domain

Self-development is a positive, goal-oriented, continuous, career-long process that should stretch and broaden Leaders beyond their institutional training and education and operational experiences as they prepare for future assignments and increased responsibilities. Leaders and Soldiers must be self-aware and assume responsibility for their own self-development through continual self-assessment and remedial actions. Self-development actions may include self-study, professional reading programs, and civilian education courses that support the individual and unit developmental goals. Self-development is a joint effort involving Soldiers, leaders, commanders, supervisors, and proponents to map efforts and set priorities to achieve maximum benefit.

8.1 Self-Development Training Concept and Strategy

The MATDEV will provide the upgrades to the units as required for the establishment of sustainment training. Training material will also be downloaded to Landwarnet for self-development training. Leaders will be capable of monitoring their Soldier's progress by use of the ALMS or equivalent. These items will be packaged so that individual Soldiers can conduct self-taught, self-paced learning. The package will monitor the Soldier's progress and level of understanding. The training will include IMI and computer based training (CBT) to provide the student with virtual hands on experience. The training will encompass both operator and maintainer training.

8.1.1 Product Lines

Product lines will consist of hardware, software, publications, courses, lessons, training aids, training facilities and management services that will provide the capabilities that trainers and Soldiers need to train in the self-development domain.

8.1.1.1 Training Information Infrastructure

Refer to Para 6.1.1.1

8.1.1.1.1 Hardware, Software, and Communications Systems

Hardware, Software, and Communications Systems. The Army Knowledge Online (AKO) infrastructure includes approved Learning Management Systems (LMS) that register students and track their progress, and provides an integrated platform for content, delivery, and management of learning via Web Based Training (WBT). The user interface is through an internet connection or use of an intranet and other standard communications protocols.

8.1.1.1.2 Storage, Retrieval, and Delivery

Digital information will be shared with the Central Army Registry (CAR), or other military training repositories as necessary, and with new repositories as they evolve through the Army Training Information Architecture (ATIA).

8.1.1.1.3 Management Capabilities

Self development training programs will utilize the Army Learning Management System (ALMS) to track student progression through lessons, exercises, and evaluations. The ALMS will be capable of downloading student academic records, tracking student progression, and sending the data back to the LWNeU (https://lwn.army.mil/). Other services will utilize their appropriate management systems to track student progression.

8.1.1.1.4 Other Enabling Capabilities

Not Applicable

8.1.1.2 Training Products

Operators and maintainers will have the same access to training as explained in Paragraphs 6.1.1.2 and 7.1.1.2.

8.1.1.2.1 Courseware

Trainers and Soldiers will have the same access to training products as explained in paragraph 6.1.1.2.1 and 7.1.1.2.1 for self-development

8.1.1.2.2 Courses

The courses are listed in para 6.1.1.2.2

8.1.1.2.3 Training Publications

All training materials, publications and user manuals are available on the MGC's info center in digital format.

8.1.1.2.4 Training Support Package (TSP)

The KMI/MGC TSP will provide training products, materials, and information that supports individual and collective tasks that will be integrated into a training and management scenario driven exercise. The multimedia TSP will be a tutorial "how to" module that permits audiences to be self-taught, wherever feasible, and will include a diagnostic test module that permits identification of Soldier training proficiency by module. Certification and sustainment training will be facilitated by the multimedia TSP left with the unit following NET.

8.1.1.3 Training Aids, Devices, Simulators and Simulations (TADSS)

Operators and maintainers will have the same access to TADSS as explained in Paragraphs 6.1.1.3

8.1.1.3.1 Training Aids

Operators and maintainers will have the same access to the same training aids as explained in Paragraph 6.1.1.3.1

8.1.1.3.2 Training Devices

Not Applicable

8.1.1.3.3 Simulators

Not Applicable

8.1.1.3.4 Simulations

Not Applicable

8.1.1.3.5 Instrumentation

Not Applicable

8.1.1.4 Training Facilities and Land

Not Applicable

8.1.1.5 Training Services

Training services required for self-development training are the same as explained in Paragraph 6.1.1.5

8.1.1.5.1 Management Support Services

Not Applicable

8.1.1.5.2 Acquisition Support Services

The TNGDEV, in conjunction with the Combat Developer (CBTDEV) and Materiel Developer (MATDEV), will explore the best possible options for contracting the development of KMI self development training products. This includes correctly conveying the KMI training strategy to the MATDEV. The MATDEV should be able to deduce from the training strategy the types of self development training products needed to support KMI training.

8.1.1.5.3 General Support Services

Not Applicable

8.1.2 Architectures and Standards Component

Not Applicable

8.1.3 Management, Evaluation, and Resource (MER) Processes Component

Not Applicable

A Milestone Annex

TRAINING DEVELOPMENT MILESTONE SCHEDULE - SHEET Annex A **PAGE 1 of 2** **Materiel Requirements Document**

SYSTEM:	ACAT	OFFICE SYMBOL	AS OF DATE
KMI CI-2	1D	ATZH-DTN	

POINTS OF CONTACT	**NAME**	**OFFICE SYMBOL**	**TELEPHONE**
MATERIEL COMMAND			
TRADOC PROPONENT	Nero Borders	IMNE-MON-LG-EM-MS	757-878-0242 DSN 826-0242
TCM-N&S	COL Roper	ATZH-IDN	DSN 780-4223
DOT	LTC Iden	ATZH-DTN	DSN: 780-6206
PD COMSEC	Ralph Jordan	SFAE-C3T-NCF	443-395-2757
SUPPORTING PROPONENTS:			

ITEM	DATE	RESPONSIBLE AGENCY/POC OFFICE SYMBOL		TELEPHONE
MNS:		ATZH-IDN	COL Roper	DSN 780-4223

SS:	06 MAY 12	SFAE-C3T-NCF	Ralph Jordan	443-395-2757
CDD:	15 AUG 06	AZTH-IDN	Al Transou	DSN 780-8050
ILSMP:		PEO-CT3-HQ	Diane Merla	732-532-0155
TTSP:	20 JUN 12	ATZH-DTN	Gerald Evans	DSN 780-8132
QQPRI:		ATZH-IDC-FB	William Dabney	DSN 780-5488
BOIP:		ATZH-IDC-FB	William Dabney	DSN 780-5488
NETP:		SFAE-C3T-NCF	Bill Ribbans	732-532-4045
CONOPS	26 MAY 10	ATZH-IDC	Stanley White	706-791-6512

COMMENTS: (Continue on reverse side if necessary)

R = Revised / Updated Approved date

C = Completed / Approved Date

D = Draft

	_ **PAGES**	
SYSTEM KMI CI-2	TRADOC SYMBOL ATZH-DTN	AS OF DATE
TRAINING PACKAGE ELEMENT/PRODUCT: Individual Training Plan/CAD/POI/Course Start Date		

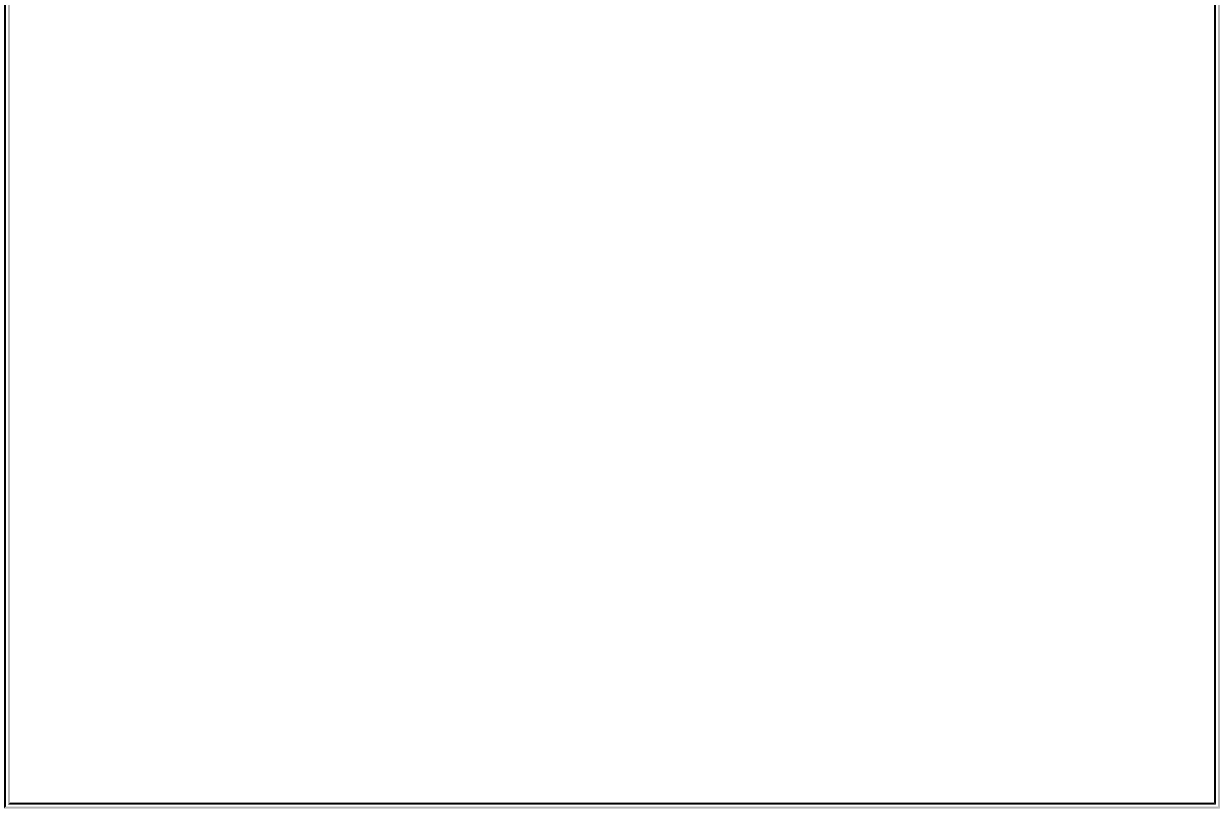
LEGEND:	MILESTONES BY QUARTER															
	FY13				FY14				FY15				FY16			
	1Q	2Q	3Q	4Q	1Q	2Q	3Q	4Q	1Q	2Q	3Q	4Q	1Q	2Q	3Q	4Q
MGC Course		5		1	6		3		2		4				8	
				7												

NOTE: All dates are estimated based on a 4QFY14 FUED

COMMENTS: (Continue on reverse side if necessary)

1. CAD
2. POI
3. ITP
4. Course Start - 3QFY15
5. NET - 4QFY14
6. FUE - 4QFY14
7. IOC
8. FOC

NOTE: All dates are estimated based on a 4QFY14 FUED



B References

Army Learning Policy and Systems, TRADOC Regulation 350-70, 6 December 2011.

Capability Development Document (CDD) for the Key Management Infrastructure (KMI) Capability Increment 2 (CI-2), dated 15 August 2006.

Concept of Operations (CONOPS) for the Transition to the Key Management Infrastructure (KMI) Increment 2 (CI-2), dated 26 May 2010.

U.S. Army Signal Center and Fort Gordon Distributed Learning Plan, dated September 2007.

Basis of Issue Plan Feeder Data, Client Host Only (CHO), dated September 2013.

C Coordination Annex

Organization/POC (Date)	Summary of Comments Submitted (A/S/C)			Comments Accepted/ Rejected						Rationale for Non-Acceptance - S, C
				Accepted			Rejected			
	A	S	C	A	S	C	A	S	C	
v1.2.11 Amanda L Iden 2014/07/28 - 2014/08/07	Document Accepted As Written			0	0	0	0	0	0	-
v1.2.10 Approvals - Catherine Collins 2014/07/28 - 2014/08/07	Document Accepted As Written			0	0	0	0	0	0	-
v1.2.4 Approvals - Catherine Collins 2014/05/28 - 2014/06/05	No Comments Submitted			0	0	0	0	0	0	-
v1.2 Army - USASOC 2010/08/17 - 2010/09/16	No Comments Submitted			0	0	0	0	0	0	-
v1.2 Army - USAREUR 2010/08/17 - 2010/09/16	No Comments Submitted			0	0	0	0	0	0	-
v1.2 Army - USARC G7 (US Army Reserve Cmd) 2010/08/17 - 2010/09/16	No Comments Submitted			0	0	0	0	0	0	-
v1.2 Army - US Joint Forces Command	No Comments			0	0	0	0	0	0	-

Net-C2 2010/08/17 - 2010/09/16	Submitted									
v1.2 Army - TRADOC_ARCIC 2010/08/17 - 2010/09/16	No Comments Submitted			0	0	0	0	0	0	-
v1.2 Army - TRADOC G-3/5 2010/08/17 - 2010/09/16	No Comments Submitted			0	0	0	0	0	0	-
v1.2 Army - TRADOC Command Safety Office 2010/08/17 - 2010/09/16	No Comments Submitted			0	0	0	0	0	0	-
v1.2 Army - TCM-Transportation 2010/08/17 - 2010/09/16	No Comments Submitted			0	0	0	0	0	0	-
v1.2 Army - TCM-Live 2010/08/17 - 2010/09/16	Document Accepted As Written			0	0	0	0	0	0	-
v1.2 Army - TCM dL 2010/08/17 - 2010/09/16	0	2	0	0	2	0	0	0	0	
v1.2 Army - TCM ATIS 2010/08/17 - 2010/09/16	3	0	0	1	0	0	2	0	0	
v1.2 Army - Space & Missile Defense	No Comments			0	0	0	0	0	0	-

Command 2010/08/17 - 2010/09/16	Submitted									
v1.2 Army - CYBER CoE - Signal School 2010/08/17 - 2010/09/16	No Comments Submitted			0	0	0	0	0	0	-
v1.2 Army - PEO-STRI Customer Support Group 2010/08/17 - 2010/09/16	0	1	0	0	1	0	0	0	0	
v1.2 Army - PEO Missiles and Space (IAMD) 2010/08/17 - 2010/09/16	No Comments Submitted			0	0	0	0	0	0	-
v1.2 Army - PEO Aviation 2010/08/17 - 2010/09/16	Document Accepted As Written			0	0	0	0	0	0	-
v1.2 Army - ICoE - Mil Intelligence School 2010/08/17 - 2010/09/16	1	1	0	1	0	0	0	1	0	
v1.2 Army - MSCoE - MANSCEN 2010/08/17 - 2010/09/16	1	1	0	1	0	0	0	1	0	
v1.2 Army - IMCOM 2010/08/17 - 2010/09/16	Document Accepted As Written			0	0	0	0	0	0	-
v1.2 Army - Human Resource Command										

(HRC) 2010/08/17 - 2010/09/16	No Comments Submitted			0	0	0	0	0	0	-
v1.2 Army - Future Force Integration (FFID) 2010/08/17 - 2010/09/16	23	0	0	21	0	0	2	0	0	
v1.2 Army - Field Artillery School 2010/08/17 - 2010/09/16	5	1	0	5	0	0	0	1	0	
v1.2 Army - Combined Arms Center 2010/08/17 - 2010/09/16	4	3	1	4	2	1	0	0	0	
v1.2 Army - SCoE 2010/08/17 - 2010/09/16	1	0	0	1	0	0	0	0	0	
v1.2 Army - USAACE - Aviation School 2010/08/17 - 2010/09/16	Document Accepted As Written			0	0	0	0	0	0	-
v1.2 Army - AVNCoE Aviation Logistics School 2010/08/17 - 2010/09/16	No Comments Submitted			0	0	0	0	0	0	-
v1.2 Army - ATSC TSAID 2010/08/17 - 2010/09/16	No Comments Submitted			0	0	0	0	0	0	-
v1.2 Army - ATSC Fielded Devices 2010/08/17 -	1	0	0	1	0	0	0	0	0	

2010/09/16										
v1.2 Army - ATSC 2010/08/17 - 2010/09/16	No Comments Submitted			0	0	0	0	0	0	-
v1.1 Peer - USARSO G3 2009/08/21 - 2009/09/20	No Comments Submitted			0	0	0	0	0	0	-
v1.1 Peer - TCM-Virtual (CS/CSS) 2009/08/21 - 2009/09/20	No Comments Submitted			0	0	0	0	0	0	-
v1.1 Peer - TCM-PBC/CID 2009/08/21 - 2009/09/20	No Comments Submitted			0	0	0	0	0	0	-
v1.1 Peer - TCM-HBCT 2009/08/21 - 2009/09/20	No Comments Submitted			0	0	0	0	0	0	-
v1.1 Peer - Soldier Support Institute (SSI) 2009/08/21 - 2009/09/20	No Comments Submitted			0	0	0	0	0	0	-
v1.1 Peer - PM-HBCT 2009/08/21 - 2009/09/20	No Comments Submitted			0	0	0	0	0	0	-
v1.1 Peer - PEO-STRI Customer Support Group 2009/08/21 - 2009/09/20	Document Accepted As Written			0	0	0	0	0	0	-

v1.1 Peer - PEO-EIS 2009/08/21 - 2009/09/20	No Comments Submitted			0	0	0	0	0	0	-
v1.1 Peer - ICoE - Mil Intelligence School 2009/08/21 - 2009/09/20	0	0	0	0	0	0	0	0	0	
v1.1 Peer - MSCoE - MANSCEN 2009/08/21 - 2009/09/20	No Comments Submitted			0	0	0	0	0	0	-
v1.1 Peer - MCoE - Infantry & Armor School 2009/08/21 - 2009/09/20	1	0	0	1	0	0	0	0	0	
v1.1 Peer - IMCOM 2009/08/21 - 2009/09/20	No Comments Submitted			0	0	0	0	0	0	-
v1.1 Peer - Future Force Integration (FFID) 2009/08/21 - 2009/09/20	2	6	1	2	6	1	0	0	0	
v1.1 Peer - Field Artillery School 2009/08/21 - 2009/09/20	No Comments Submitted			0	0	0	0	0	0	-
v1.1 Peer - Combined Arms Center 2009/08/21 - 2009/09/20	3	7	0	3	7	0	0	0	0	
v1.1 Peer - SCoE 2009/08/21 -	No Comments			0	0	0	0	0	0	-

2009/09/20	Submitted									
v1.1 Peer - USAACE - Aviation School 2009/08/21 - 2009/09/20	Document Accepted As Written			0	0	0	0	0	0	-
v1.1 Peer - AVNCoE Aviation Logistics School 2009/08/21 - 2009/09/20	No Comments Submitted			0	0	0	0	0	0	-
v1.1 Peer - ATSC 2009/08/21 - 2009/09/20	No Comments Submitted			0	0	0	0	0	0	-
v1.1 Peer - Army Research Laboratory (ARL) 2009/08/21 - 2009/09/20	5	2	1	3	2	0	2	0	1	
v1.1 Peer - Army Material Command (AMC), G3 2009/08/21 - 2009/09/20	No Comments Submitted			0	0	0	0	0	0	-
v1.1 Peer - MCoE - Armor School 2009/08/21 - 2009/09/20	0	8	0	0	5	0	0	3	0	
v1.1 Peer - AMEDD Center & School 2009/08/21 - 2009/09/20	Document Accepted As Written			0	0	0	0	0	0	-
v1.1 Peer - AMC G-8 2009/08/21 - 2009/09/20	No Comments Submitted			0	0	0	0	0	0	-

v1.1 Peer - FCoE-ADA School 2009/08/21 - 2009/09/20	1	0	1	1	0	1	0	0	0	
v1.1 Peer - 428th BDE 2009/08/21 - 2009/09/20	No Comments Submitted			0	0	0	0	0	0	-

Key
Completed Review with Comments
Completed Review, No Comments
Active Review Occurring

DEPARTMENT OF THE ARMY
HEADQUARTERS UNITED STATES ARMY CYBER CENTER OF EXCELLENCE
AND FORT GORDON
506 CHAMBERLAIN AVENUE
FORT GORDON GEORGIA 30905-5735

AZTH-DT 1 August 2014

MEMORANDUM FOR Commander, Army Training Support Center (ATSC), Systems Training Integration and Devices Directorate (STIDD), Army Modernization Office, (ATTN: ATSC-STIDD/Mr. Nero Borders), Fort Eustis, VA 23604-5166

SUBJECT: Key Management Infrastructure (KMI) Capability Increment 2 (CI-2) System Training Plan (STRAP) Approval Memorandum

1. References:

a. Army Regulation 350-1, Army Training and Leader Development, 4 Aug 2011.

b. TRADOC Regulation 350-70, Army Learning Policy and Systems, 6 Dec 2011.

c. TRADOC Regulation, 71-20, Concept Development, Experimentation, and Requirements Determination, 6 May 2009.

d. KMI Capability Production Document (CPD), Version 3.0, 16 Dec 2009.

2. The KMI CI-2 STRAP is approved. Approved STRAP will be posted to the Central Army Registry website: https://atiam.train.army.mil/catalog/catalog/search.html

3. Point of contact for this memorandum is Mr. Gerald F. Evans Jr at (706) 791-8132, DSN 780-8132 or gerald.f.evans4.civ@mail.mil.

IDEN.AMANDA.L.1[illegible].1046127214

AMANDA L. IDEN
LTC, SC
Deputy Director, Directorate of Training

Approval Memo